MIT SAP Security & GRC Process : 1. New or Amended Roles

Massachusetts Institute of Technology

Risk Owner

FYI EMAIL

14 MAINTAIN RISK AWARENESS

FYI EMAIL

Role Owner

START

1.a Initiate proposal for New / Amended Roles

RT NEW TICKET

FYI EMAIL

5 Approve Role Build / Amendment

9 Approve Role Build / Amendment **In PROD**

13 Close Out RT TICKET

All paperwork

R/3 Security Admin

START

1.b Initiate proposal for New / Amended Roles

6 Process 3 Role Provisioning IN TEST

FROM 7, 11

10 Process 3 Role Provisioning and QA IN PROD

BA / BSA

2 Role Design review and GRC-ARA Simulations

New SOD Risks identified ?

NO

YES

4 Finalize Role Design / Redesign and run GRC-ARA

GRC-ARA report

NEW ROLE DESIGN

ROLE MINI-SPEC

TEST PLAN

FROM 7, 11

3 Process 2 Mitigation Analysis & Design

Email -ready for test

NO Some minor fixes are required

USER LEVEL GRC-ARA report

USER LEVEL GRC-ARA report

FILED

7 SAP TEST Test New/Changed Role and run GRC-ARA

Test OK ?

YES

NO Additional SOD Risks Identified

STEP 3

11 SAP PROD GRC-ARA review And Support USER

Test OK ?

YES

NO Additional SOD Risks Identified

STEP 3

NO Some minor fixes are required

STEP 6

Feedback and TEST RESULTS

Feedback

End User

8 SAP TEST Test the role

12 SAP PROD Confirm role works

Process 1: New or Amended Roles

The "New or Amended Role" process is for the scenario where a new or amended business role is needed, and includes the high-level steps for initial investigation, design, development and GRC Access Risk assessment.

The requirement SAP Access Role maintenance can be identified during the following business events, with the first two being the most frequent and represented in the flowchart. The process for the other triggering events is almost the same, with any differences documented in the text.

1. Departmental reorganization.
2. New or changed job duties within a department.
3. New SAP functionality which is not expected to be included in common roles but is needed for several users with different access and does fit into an existing role. This may be:
    - Small changes, for extra functionality in existing applications
    - Larger, project-related changes where a whole new application is rolled-out, and probably multiple SAP Access roles.
4. Audits, Compliance and other reviews – this would be less common.
5. SAP Access role redesign / tidy-up (triggered from technical reviews).
6. Removal of functionality from roles – (no SOD risk issues).

Roles & Responsibilities for Process 1:

- **Risk Owner :** Maintains awareness of role changes and potential for new risks
- **Role Owner :** Initiates proposals for role changes, approved role changes, closes out role change process
- **BA / BSA :** **Involvement in several steps**
    - Performs preliminary role change analysis
    - Creates role design / redesign documentation and test plan
    - Tests new roles in TEST – including GRC-ARA simulation

  - Supports end-user in Production.

- **R/3 Security Admin:** Builds roles and provisions role (see process 3).
- **SOD Coordinator:** Indirectly involved if there is any Mitigation requirements – see Process 2.
- **GRC Admin:** Indirectly involved if there is any Mitigation requirements – see Process 2.
- **End User:** Test their User in SAP Production.

Reports available to support the Process 1:

Rept. 5	R/3 SUIM	Roles by Role Name
Rept. 6	GRC	User to Role relationship
Rept. 7	GRC	Role relationship with User
Rept. 8	R/3 SUIM	Users by User ID
Rept. 9	GRC	Count of Authorizations
Rept. 10	GRC	Action Usage by User, Role, Profile
Rept. 12	GRC	User Level access analysis
Rept. 13	GRC	User Level access analysis – simulation with added / removed actions, roles, profiles.
Rept. 14	GRC	Role Level access analysis
Rept. 15	GRC	Role Level access analysis – simulation with added / removed actions, roles, profiles.

TCODE SU01D	Display User information – with Roles and Profiles tab

The following report are also available, but will be less frequently used in the MIT environment:

Rept. 16	GRC	Profile Level access analysis
Rept. 17	GRC	Profile Level access analysis – simulation with added / removed actions.

Process 1: New or Amended Roles - Detailed Steps

P.1 STEP	Business Role	Responsibility / Action	Output	Details
1	Role Owner	Initiate proposal for New/Amended Roles.	• Email to BA/BSA and Risk Owner, SAP Security Admin and MIT Audit • RT Queue – new task	a. Role Owner identifies a potential need for a new role due to : • Departmental Reorganization – new roles are needed to reflect completely new, permanent job duties, and old roles probably can be deactivated. • New or changed job duties – may be combined roles or split role or just completely new. This is less likely where provisioning is managed with Composite roles which can have existing roles added / removed without the need for a new role. • New SAP functionality which does not easily fit into an existing role. b. Role Owner communicates (email) potential need to BA/BSA and Risk Owner. c. The requirement may be triggered from a technical role redesign proposed by SAP Security Admin. **Note** that MIT's has made more use of "**composite roles**" in the redesigned VPF access. The composite role is where several roles are linked together to represent a job position or a specific user's duties. • So some minor User access changes can be managed by adding or removing roles from the composite role. • This would be identified by the Role Owner in simpler cases, or by the BA/BSA for more complicated cases – see step 2.

P.1 STEP	Business Role	Responsibility / Action	Output	Details

2	BA/BSA	Role Design review and GRC-ARA simulations	• GRC-ARA Risk simulation reports
			• For existing risks, assessment of existing Mitigation Controls to new tcode combination.
			• If new Risks, kick-off a full risk assessment (see next step = Process 2).
				a. For major changes, e.g. complete business reorganization or new major multi-role applications being rolled out, there will always be a need for everyone to be involved, like the SOD project had.
				b. For minor changes, the BA/BSA will **review the current role design (GRC and SUIM reports)** and decide if any new Roles are necessary to achieve the business changes. Where there are any new action tcodes (create, change, post etc.), or new combinations of tcodes due to composite role changes, a GRC-ARA SOD analysis is required for:
				  • The proposed new / changed role
				  • The users for whom the change will be made
				• The GRC-ARA simulation can use the current user in PROD, plus any tcodes (entered) or existing roles (in DEV, TEST/QA or PROD).
				• SAP R/3 Security Admin may need to advise on additional authorizations (permission level) which may reduce the risk.
				• The BSA may need to advise on alternative tcodes (actions) and standard SAP equivalents of custom "Z" transactions.
				• The proposed design can be workshopped, including bringing up any SOD issues and recommendations for mitigation. (See details in **Process 2: Mitigation Analysis**).
				c. In defining design requirements for the request, the BA/BSA works with the Role Owner and Risk Owner.
				  • to mitigate risks and SODs wherever possible,
				  • reaching out to the GRC Analysis Team when input is required
				d. Check any existing Mitigation Controls related to the current role, and check the detail of the new tcode combinations. It is possible the existing Mitigation Control does not fully cover the new tcodes.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
3	BA/BSA Risk Owner Role Owner SOD Coordinator	Mitigation Analysis	See Process 2 Flowchart for details	**Also, see Flowchart for Process 2 for more details.** a. Mitigation analysis is required where : • New SOD Risks are reported • Existing SOD Risks remain, but are changed due to the new tcodes • New "Critical" transactions (actions) are reported. b. Detailed SOD Risk analysis will confirm if : • risk is low level and is acceptable, or • existing mitigation could apply / still applies, or • a new mitigation control can be defined, or • a new mitigation process may need to be developed o new report o system enhancement o system configuration change o additional SAP Access restrictions – permission level o new manual process. c. The output of this step will be one or more role redesigns and potentially a new Mitigation Control if the Risk remains after the role redesigns. Note the Risk may have been avoided due to "Remediation" : • Several roles and related user assignments were changed • The tcode causing the issue was put in a "FireFighter" role.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
4	BA/BSA	Finalize role Design / Redesign ad run GRC-ARA simulation	• Role Mini-Spec • New Role Design spreadsheet • GRC-ARA Simulation reports • Test plan and test cases	a. Prepare Role Design / Redesign documentation – including : • Composite Role changes ○ Existing Composite Role: roles to be added or removed ○ New Composite Role to be created and its roles ○ Changes in assignment of Composite Roles to User • Single Role changes ○ New Single Roles ○ Transaction Codes (Actions) to be added or removed ○ Authorizations (Permissions) to be added, removed or changed • FireFighter roles for back-up of new/amended role – ○ New FireFighter roles ○ Existing FireFighter roles - changes to tcodes and other authorizations. ○ Assignment of new FireFighter Roles to Users (see Process 4) • Mitigation documentation (part of Process 2: Mitigation Analysis). • **GRC-ARA SOD Risk Analysis Role and/or User simulation Report 13 and 15**, where possible. b. For major redesigns or new complex applications, the supporting documentation must include full GRC-ARA analysis – probably on the new Roles built in DEV. This step is not included in the flowchart.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
5	Role Owner	Approve Role Built / Amendment	a. Email SAP Security Admin b. SAP Mini-Spec for Access Change request	a. Give the initial go ahead for new/amended role. • Check GRC-ARA simulation results (printed report) • Review detailed Mini-Spec / SAP Access Change request • Email SAP R/3 Security Admin ○ Give approval to proceed and RT # ○ Include New Role Design document (for new roles) ○ Include Role Mini-Spec (for new / amended roles)
6	SAP Security Admin	Process 3: New Users and User Role Provisioning In TEST system	• Email to BA/BSA when complete • Amended Role • Saved copy of current role • Update RT Ticket	a. IS&T have a process for managing RT tickets, their prioritization and execution, including a QA review prior to approval of transports going into Production. The details of this process are not documented here. b. Here are the action steps specific to the Role Change requests: • Review all supporting documentation for completeness and for correspondence with the RT ticket description. • **Determine if this request involves the already redesigned roles, or the old roles. For amending original roles, proceed with the old provisioning process.** • Identify any potential overlap with the RoleDB • For any new roles, determine naming convention and check the proposed assignment to composite roles (and related users) or users. • Build or amend the role in SAP Development, move it to TEST/QA, and then assign to a test user, alias or to a composite role. ○ Take a safety copy of any existing role being amended ○ This can be iterative where role design is incomplete or incorrect. • Perform basic unit testing. • Advise BA/BSA the new / amended role is ready for testing

P.1 STEP	Business Role	Responsibility / Action	Output	Details
7	BA/BSA	Check role build, GRC-ARA and assist user with testing	• GRC-ARA simulation reports • Functionality test results • Updated RT-related documentation	a. Check role build / amendments in TEST/QA system • **SUIM report** b. Run GRC-ARA SOD Risk simulation Report 15 on the Role & Report 13 on all Users to be assigned the role. • Use the new/amended Role from TEST/QA system, User from PROD system. • If any new risks are reported, check the reason and revisit the Mitigation process (Step 3). c. Assist the business User with testing the role functionality in SAP TEST/QA system (see Step 8.) d. Update RT-related documentation with test results. e. Email Role owner when business user has accepted the changes.
8	End user and/or BA		• Functionality test results	a. Test the new/amended role functionality in TEST/QA system b. If there are any issues : • Go back to Step 6 for minor changes (e.g. a previously unidentified permission is required for a new tcode). • Go back to Step 4 for any major changes – e.g. additional or alternative tcodes are required. [Not shown on flowchart].
9	Role Owner	Review simulations - if no issues, approve move to SAP Production.	• Email to SAP Security Admin • Updated SAP Access Change request form • Update RT Ticket	a. Review all the paperwork, including Simulation reports. b. Follow-up any issues. c. If all is good, send email to SAP R/3 Security Admin to request promotion to PROD. • Include any special requests – e.g. staggered roll-out to several users at a time, which is more difficult when using Composite Roles.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
10	SAP Security Admin	Role provisioning and Transport QA review	• Email to BA/BSA and Role Owner when complete • Update RT Ticket	a. IS&T have a process for managing RT tickets, their prioritization and execution, including a QA review prior to approval of transports going into Production. The all the details of this process are not documented here, just the ones relating to the roles. ○ Ensure roles in DEV and TEST/QA are matching ○ Ensure existing role to be amended in PROD is backed up ○ Check all paperwork for release is complete, coordinate with BSA as appropriate. ○ Request Transport QA review and promotion to PROD ○ Check transports were imported and briefly review roles. b. Email status to Role Owner • **NOTE:** It is also possible there is a need to tweak the RolesDataBase interface with SAP Production – i.e. stop a profile coming over for the users affected by the role changes.
11	BA/BSA	Run User level GRC simulation for all users expected to be assigned the new role. Potential risk that RolesDB profiles causes an issue see Step 17.	• GRC-ARA simulation reports.	Repeat of step 7 – except BA/BSA does not have access in PROD so cannot confirm anything is working.
12	End user	Test role functionality in Production	• Functionality test results	Repeat of Step 8.

P.1 STEP	Business Role	Responsibility / Action	Output	Details
13	Role Owner	If no issues, close out the change request	• Email to SAP Security Admin • Updated RT • Signed off SAP Access request?	a. RT ticket can be closed out b. Courtesy email to all involved c. Paperwork check (or confirm with BA/BSA) – all is filed d. Mitigation: additional coordination required if new / amended Mitigations were required – see **Process 2: Mitigation Analysis.**
14	Risk Owner	Maintains awareness of role changes and their implementation.		Maintains general awareness of SAP access within business area. Look out for any new issues at next SOD Review.